

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	1703	713/187,188,200.ccls.	USPAT	OR	OFF	2005/03/04 10:10
L5	959	L4 and file	USPAT	OR	OFF	2005/03/04 10:10
L6	15	L5 and detect\$4 and file with (truncat\$4 re\$1nam\$4) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:20
L7	8	L5 and detect\$4 and file with (perm\$6 own\$6) with (chang\$4 modif\$7) and file with detect\$4	USPAT	OR	OFF	2005/03/04 12:26
L13	26	detect\$4 and (permission access) with (bit header) with (chang\$4 modif\$7) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:11
L14	8	detect\$4 and (permission access) with (bit header) with (chang\$4 modif\$7) with (detect\$4 output\$4) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:13
L16	127	detect\$4 and (permission access) with (chang\$4 modif\$7) with (detect\$4 output\$4) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:14
L17	127	detect\$4 and (permission access) with (chang\$4 modif\$7) with (detect\$4 output\$4) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:14
L22	10	detect\$4 and (chang\$4 modif\$6) with (group adj (permission own\$6 access)) and file with detect\$4	USPAT	OR	OFF	2005/03/04 11:26
S1	496	crosbie.in. kuperman.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/03/02 16:15
S2	20	S1 and file	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/03/02 16:38
S3	1703	713/187,188,200.ccls.	USPAT	OR	OFF	2005/03/02 16:39
S4	959	S3 and file	USPAT	OR	OFF	2005/03/02 16:39
S5	600	S4 and detect\$4	USPAT	OR	OFF	2005/03/02 16:39
S6	146	S4 and detect\$4 and file with detect\$4	USPAT	OR	OFF	2005/03/04 10:10
S7	1	"4975950".PN.	USPAT; USOCR	OR	OFF	2005/03/03 11:07

1. A method of detecting critical file changes, comprising:
 - Reading events representing various types of system calls;
 - Routing the event to an appropriate template, the event having multiple parameters;
 - Filtering the event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event; and
 - Creating an intrusion alert if an event is output from said filtering step.
2. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that the permission bits on a file or directory were changed.
3. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that a file was opened for truncation.
4. The method of claim 1, wherein said filtering step outputs an event if the parameters indicate that ownership or group ownership of a file has been changed.
5. The method of claim 1, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to.
6. The method of claim 1, comprising configuring templates based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.
7. A method of detecting critical file changes, comprising:
 - Reading events including encoded information representing system calls;
 - Routing the event to an appropriate template based on the encoded information;
 - Filtering the event as either a possible intrusion based on the encoded information and either dropping the event or outputting the event; and
 - Creating an intrusion alert of an event is output from said filtering step.
8. The method of claim 7, wherein said filtering step outputs an event if the encoded information indicates that the permission bits on a file or directory were changed.
9. The method of claim 7, wherein said filtering step outputs an event if the encoded information indicates that a file was opened for truncation.
10. The method of claim 7, wherein said filtering step outputs an event of the encoded information indicates that ownership or group ownership of a file has been changed.
11. The method of claim 7, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to.

12. The method of claim 7, comprising configuring templates based a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.